Consolidated Technology Services • WA

Service Improvement
Identity Management Service

January 29, 2013

Business Driver

Washington State agencies are seeing an increase in the use of 'cloud providers'.

This raises challenges in the areas of:

- ensuring adequate security (authentication, authorization, data security)
- enabling ease of use (eliminating need to maintain separate credentials for each application, ability to self-provision password resets)
- limiting administrative load for technicians (eliminating duplication of administrative tasks)
- standardizing authentication and authorization processes across various state-agency-supported applications (allowing application developers to focus on business logic).

These challenges have highlighted the value of an ***Enterprise Identity Management (IdM)*** service.

Overview and Potential Benefits

An IdM generally has three components:

1. ***Identity*** – A database (identity store) containing 'vetted' user identity information
2. ***Authentication/Authorization*** – A process to authenticate a request against the identity store and determine authorization for specific functionality.
3. ***Lifecycle management*** – A process that controls how an identity comes into existence in the store, how it is maintained, and how it is removed. This process also provides for auditability.

Every secure application has some form of IdM, either internal or via 'federation' with an external IdM.

An 'Enterprise' IdM can be shared by all entities that are operating on the same network. It can be logically extended (federated) with trusted entities outside the network (in the cloud).

The benefits of an 'Enterprise' IdM service include:

- Increased security – security-related activities are not scattered across a variety of IdMs, but are centralized and standardized, making accountability much easier to achieve.
- Increased convenience – users can learn a single set of credentials and use them wherever they are authorized to do business as part of their job.
- Reduced cost – an 'Enterprise' IdM service can scale, eliminating the need for multiple instances of redundant infrastructure.
- Increased standardization – applications developed by different state agencies can share a common authentication/authorization process
- Reduced support load – Information Technology staff time spent managing administrative tasks is reduced.
- Increased accuracy – Automated work flows and policies can be implemented to reduce human error in granting authorization to resources.
- Improved auditability – a central source exists to account for authentication and authorization activities.

Effort to Deploy and Support:
Washington State began implementation of an Enterprise IdM in 2001. This service is known as Enterprise Active Directory (EAD).

In the decade since it was established, 58 agencies have joined the EAD community. However, 8 agencies (along with a handful of boards and commissions) have not joined, citing level of effort, cost, and security concerns.

EAD has provided the ***identity store*** component of IdM through use of the Active Directory (AD) product. Each agency owns and administers an AD domain (data store), or uses CTS' Shared Domain service. These are joined into a 'forest' with a common 'root', which is maintained by CTS. In this manner, data is replicated across member AD domains and thus made available to all EAD members.

EAD has provided the ***authentication/authorization*** component through Windows Authentication Services. This capability was recently enhanced through implementation of Active Directory Federation Services (ADFS) in the 'root' to extend EAD credentials to trusted applications in the cloud.

The IdM component missing from EAD, ***lifecycle management***, is now being considered via implementation of Forefront Identity Manager (FIM) – See the associated FIM Conceptual Design. This gap is currently being filled by various manual processes at the member agency level.

NOTE: The referenced FIM Conceptual Design concerns itself with the infrastructure, licensing, and support requirements of FIM. However, in order to ***make FIM implementation successful***, there is much work required in the areas of governance, administration, and standardization. FIM will require a much more tightly-coupled EAD environment. For example, 'authoritative sources' must be identified for key data elements, which FIM will then synchronize to all data stores. Another example is that roles and responsibilities must be standardized across the environment so they can be automated by FIM as 'workflows'. Also, as a result of the current decentralized administration, existing data stores contain a significant amount of out-of-date or otherwise inaccurate data, and suffer from inconsistent use of data fields. These must be reconciled.

EAD membership commitment to this body of effort must be obtained, and a governance mechanism must be put in place (such as the EAD Steering Committee that was so active in standing up EAD).

Even given an implementation of FIM, there remain several factors limiting full realization of IdM benefits through EAD:

1. Not all state entities have joined (see above).
2. Many member agencies have closed firewall ports between their AD domains and other member's, increasing the complexity and time required to make new applications work with EAD.
3. Some member agencies have used network address translation (NAT) on their domains, rendering them 'invisible' to the rest of EAD, making auditing and accountability impossible.

Recommendation
As EAD has been promulgated as the Standard IdM for State agency use (see OCIO Standard 183.20), the recommended path to service improvement for Identity Management in the State of Washington includes:

- Adoption of EAD by all Executive Agencies.

- Standardization, centralization, and automation of the ***lifecycle management*** process using FIM.
- Implementation of standardized network addressing and firewall policies.

CTS Responsibilities:

- Lead process to standardize network and firewall configuration.
- Lead process to standardize the EAD schema catalog (data store layout).
- Lead process to standardize lifecycle management policies and workflows.
- Assume central responsibility for Lifecycle Management. Acquire and deploy FIM to automate processes and enforce standardization of identity store, and provide enhanced auditability.

Agency Responsibilities:

- Participate in standardization and workflow/policy activities.
- Implement necessary changes to in their agency domains.
- Comply with finalized standards.
- Commitment to migrate to EAD within a negotiated timeline.

Costs:

The costs for infrastructure acquisition and deployment for FIM can be found in the associated FIM Conceptual Design.

The costs to develop and implement the governance and standards required to complete the EAD IdM solution are almost entirely comprised of FTE-hours, and are not estimated in this document. However, the expectation is that they are not insignificant, especially for agencies yet to come into EAD.

Due to the nature of the governance, standards development, and EAD join efforts, it is expected that achieving a full Enterprise IdM will be a long-term 'program', rather than a short-term project.